Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 40 (2011) 5545-5548

ISSN: 2229-712X

A medical image encryption and decryption approach using chaos and LSB

I. Bremnavas[1], B.Poorna[2] and G.R.Kanagachidambaresan[3]

[1]Department of Computer Applications, Anna University of Technology, Trichirappalli – 24

[2]Department of Computer Applications, Easwari Engineering College, Chennai – 89

[3]Anna University of Technology, Trichirappalli – 24.

ARTICLE INFO

Article history:

Received: 15 September 2011;

Received in revised form:

14 November 2011;

Accepted: 22 November 2011;

Keywords

Encryption,
Decryption,
Chaotic,
Henon map,
Cryptography,
Steganography,
LSB,
Matlab.

ABSTRACT

Steganography is a captivating area of research in the new modern world. Steganography is a form of covert communication in which a secret message is invisible within a carrier message. Various image Steganography techniques have been proposed. The user data should be made secret in order to have the user's privacy and security. This novel algorithm represents the encryption and decryption of medical data of the patient and the patient's medical image using LSB and chaotic systems. In this paper, investigate diverse Steganography techniques and tools. The chaotic signal generation and the result analysis are done by using the Matlab 7.10.

Introduction

The goal of Steganography is to camouflage the very presence of communication, making the true message not detectable to the observer. Steganography have to give high imperceptibility, security level and payload. The security threats such as eavesdrop and illegal access to the secret messages causes overriding of the users privacy hence the users data should be protected by using this novel algorithm. This work is framed in such a way that it prevents the user's data from all sorts of attacks such as brute force and other attacks. Steganography is part of the encryption and decryption technique, the message can be sent without taking any intimation.

Steganography technique adapts image, sound and text as a cover image to send the message. LSB (least significant bit) is one of the common ways for data Steganography in text. Steganography technique based on unsystematic data embedding in text LSB has been proposed in which embedding a character. [1, 2]

Many cryptographic algorithms based on chaos theory are presented till now [3] and some of them are somehow employed in way that is capable of image encryption and decryption addition to the text encryption and decryption. One of the main advantages of chaotic system's realization is facilitated key management approach because this method only needs to protect and secure transmission of secret key (parameters and initial values of chaotic system), which has a little volume and therefore not only a little memory is needed to maintain it but also there is more confidence during its transfer.

LSB and Chaos Implementation:

The classic LSB Steganography embeds message into cover medium by using message bit stream to replace the cover medium least-significant bit (LSB) directly. There are several types of LSB embedding methods. Currently three effective methods in applying Image Steganography: LSB Substitution, Blocking, and Palette Modification. In this paper focus only LSB (Least Significant Bit) Substitution process. One of the techniques used in Steganography to hide data behind images is called the least-significant bit (LSB) substitution wherein the LSB of each byte of the pixel of the text raster data is replaced with the single bit of the data to be hidden. LSB Substitution is the process of modifying the least significant bit of the pixels of the carrier image. LSB Steganography that replaces the least significant bits of the host medium is a widely used technique with low computational complexity and high insertion capacity. Here the paper proposed to implement LSB Substitution used to encrypt and decrypt for patient text detail. [4, 5]

The advantages of chaotic signals are the compassion to the primary conditions meant that a minor change in primary amount will cause a significant difference in subsequent measures. Apparently accidental feature in comparison with productive accidental natural number in which the range of the numbers cannot be produced again, the technique used for producing the accidental number in algorithm based on the chaotic function. Unpredictable and non-linear: This means they are sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes. [6].

The First Stage of this paper focussed on the patient medical details are encrypted and decrypted used in Least Significant Bit Steganography Technique. Another important algorithm in steganography is Chaos. The second stage of work is focused in to encrypt and decrypt the patient image used this chaos algorithm. It is a phenomenon that occurs in nonlinear definable systems sensitive to initial conditions and has a pseudo-random behaviour.

Tele:
E-mail addresses: jmcnavas@gmail.com, poornasundar@yahoo.com

An important characteristic that has caused this phenomenon to take into consideration for many cryptographic systems is being definable despite of its pseudo-random behaviour. Due to pseudo-random behaviour, the output of the vision system seems random in attackers' view, while in receiver's view, the system can be defined and decryption is possible. One of the vastly used chaotic two dimensional systems is Henon map.

Henon Map:

The Henon map is a prototypical two dimensional invertible iterated map represented by the state equations with a chaotic attractor. The chaotic Henon mapping has been proposed as a method of generating pseudo-random sequences [7, 8]. The two-dimensional Henon map is defined as follows:

$X_{n+1} = 1 + y_n - \alpha x_n^2$ --------- (1)

$Y_{n+1} = \beta x_n$ --------- (2)

Where 'α' and 'β' are constants. With initial point (x_0, y_0). The pair (x, y) is the two dimensional state of the system. When $\alpha = 1.4$ and $\beta = 0.3$, the system is in chaotic state. Henon map possesses a strange attractor, for any value of x_i; yi in the Sequence the point quickly converges to this attractor and remains on it during the iteration that follows. [9, 10]

Schematic Diagram:

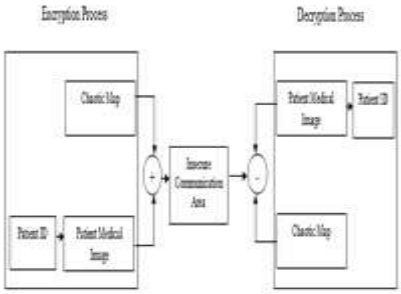

Fig.1. Schematic diagram of the proposed encryption and decryption scheme

Work flow Diagram:

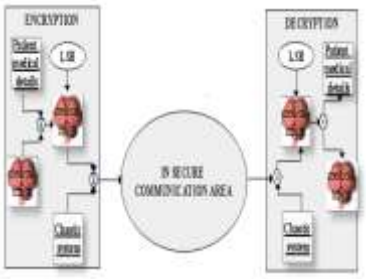

Fig.2. Workflow diagram of the proposed encryption and decryption scheme

Simulation and Results:

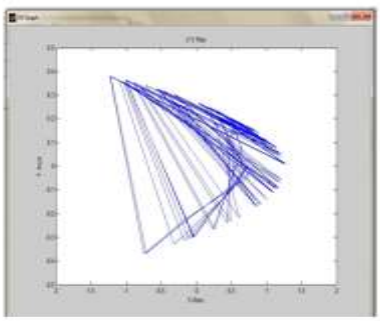

Fig 3: Henon sequence between -0.5 to 0.5

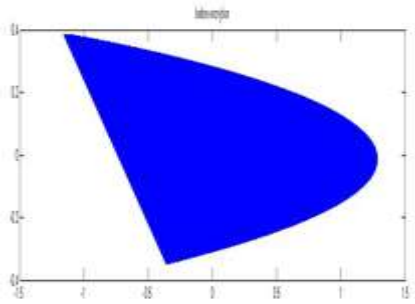

Fig. 4 depicts the phase filled Henon map in which the chaotic region is shown in the raw chaotic map generated through the matlab simulator

Fig 5.Image before Encryption

Fig. 6 Image after Decryption

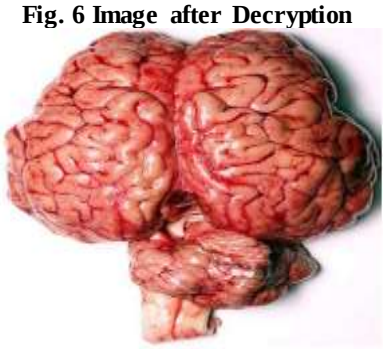

Fig 7. Image before Encryption

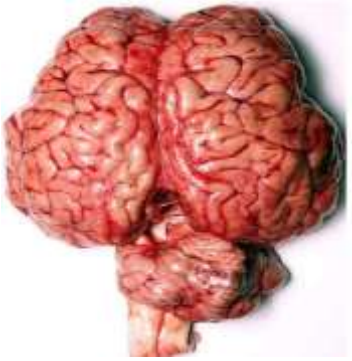

Fig.8. Image after Decryption

A heart image of size 300*300 and a brain image of 315*448 are used as the image signal and it is encrypted both with the noise and without noise signals and decrypted using the Henon sequence. The medical images of heart and brain of

different size is used. The algorithm works for various sizes of medical images. In the decryption phase, the receiver receives the encrypted medical image and filters the chaotic signal.

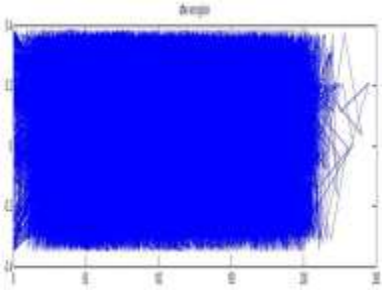

Fig 9: signal after encryption

Figure 9. The patient ID and patient medical Image is encrypted using LSB and Chaos.

Conclusion:

A new method was proposed for medical image encryption and decryption, in this paper using the LSB and chaotic signals and this caused a kind of scattering format for the data embedding place in the image, as they are randomly selected. This novel algorithm represents the encryption and decryption of medical data of the patient and the patients' medical image using chaotic based systems. The chaotic signal generation and the result analysis are done using the Matlab 7.10.

Reference:

[1] N. F. Johnson and S. Katzenbeisser, "A survey of Steganographic techniques" Information Hiding, S. Katzenbeisser and F. Petitcolas, Eds. Norwood, 2000, MA: Artech House, pp. 43–78.

[2] D. Kahn, "The history of steganography", *Proc. of the first Workshop on Information hiding*, 30 May-1 June 1996, Cambridge, UK, pp 1-5, Lecture Notes Computer Science. (Springer-Verlag), 1174.

[3] Wayner, p., "Cryptography with Choatic Map", Image and Fractal, 2002, pp.1312-1323.

[4] Westfeld, A. PFitzman, "Attaks on Steganography Systems," Proc. 3rd Int1 Information Hiding Workshop, Springer-Verlog, 1999, pp. 61-76.

[5].Ankita Agarwal, Sherish Johri, Vikas Tyagi "Method for Image Steganography using LSB approach"

[6] Ponomarenko VI, Prokhorov MD. Extracting information masked by the chaotic signal of a time-delay system. Phys Rev E 2002; 66:026215–21.

[7] M. Henon, "A Two-Dimensional Mapping with a Strange Attractor," *Communication in Mathematical physics*, vol. 50, 1976, pp. 69–77.

[8] R. Forre, "The Henon Attractor as Key Stream Generator," *Abstracts of Eurocrypt 91*, 1991, pp. 76–80.

[9] A.S. Alghamdi, H. Ullah, M. Mahmud, and M.K. Khan, "Bio-Chaotic Stream Cipher- Based Iris Image Encryption," *Proceedings of the International Conference on Computational Science and Engineering*, 2009, pp. 739–744.

[10] X.Y. Yu, J. Zhang, H.E. Ren, G.S. Xu1, and X.Y. Luo, "Chaotic Image Scrambling Algorithm Based on S-DES," *Journal of Physics: Conference Series*, vol. 48, 2006, pp. 349–353.

Algorithms and Diagrams:

LSB Algorithm for Encryption:

I/P: Medical image, M and Medical data, D

O/P: Encrypted image, E

Step 1 : Convert the medical data, D of the patient to the UTF code format, U.

Step 2 : Convert the UTF code, U in to 8-bit binary format data, B.

Step 3 : Divide the medical image, M of the corresponding patient into 8, 16, 32 - blocks Irrespective of the medical image size.

Step 4 : Add the binaries medical data i.e. binary data, B into the medical image, M Using the random number generation process which creates an Encrypted image, E.

LSB Algorithm for Decryption:

I/P: Encrypted image, E

O/P: Medical data, D

Step 1: Divide the encrypted medical image, E into 8, 16, 32 - blocks respective of the data size.

Step 2: Extracted the medical data, D from the binary 8, 16, 32 blocks using chaos system.

Step 3: Convert the binary data, B into UTF value, U.

Step 4: Convert the UTF value, U into text format.

Step 5: The data is extracted from the medical image.

Chaos Algorithm for Encryption:
I/P: User Image, I
O/P: Encrypted signal, ES
Step 1: Generate chaotic sequence (H) using Henon map using following equations

$$X_{n+1} = 1 + y_n - \alpha x_n^2$$
$$Y_{n+1} = \beta x_n$$

Step 2: Convert the user image, I to pixel array (P) format suitable for encryption process.
Step 3: Plot the generated Henon sequence $H\{x_0, y_0, a\}$ and obtain raw Henon map without any user data.
Step 4: Encrypt the image signal (P) with Henon sequence signal (H) in the chaotic region of the Henon sequence to get encrypted signal, ES.
Step 5: Transmit the encrypted signal (ES) in open communication channel.

Chaos Algorithm for Decryption:
I/P: Encrypted Signal, ES
O/P: User Image, I
Step 1: Receive the encrypted signal, ES from the open communication channel.
Step 2: Generate the Henon sequence, H using the Henon equations
Step 3: Subtract the received encrypted signal, ES with the raw Henon signal, H to obtain user image signal, IS.
Step 4: Convert the resultant image signal, IS into image, I.

Table 1. The patient details to be encrypted decrypted using LSB Algorithm

Patient Id	Patient Name	Patient Detials	Age	Sex
BM768	XXX	FVHEART	34	M
HD89	AAA	UVBRAIN	18	F

Table 2. The patient details to be decrypted using LSB Algorithm

Patient Id	Patient Name	Patient Detials	Age	Sex
BM768	XXX	FVHEART	34	M
HD89	AAA	UVBRAIN	18	F